

What is claimed is:

1. A system for authentication and authorization of physical equipment use comprising:
a computer network having a central computer gateway;
at least one system-access detector having a location identification, said at least one system-access detector interfacing with said central computer gateway; and
at least one client identifier unit having a client identification and located with the equipment, said client identifier unit communicating with at least one of said at least one system-access detector.
2. A system according to claim 1, wherein said location identification of each of said at least one system-access detector comprises a media access control (MAC) address and an Internet protocol (IP) address.
3. A system according to claim 1, wherein each of said client identification of each of said at least one client identifier unit comprises a MAC address.
4. A system according to claim 1, wherein each of said at least one client identifier unit further comprises:
a controller coupled with the physical equipment, said controller having means for identifying an operator of the physical equipment; and
a spread spectrum data transceiver connected with said controller, said spread spectrum data transceiver communicating data between said controller and at least one of said at least one system-access detector.

5. A system according to claim 4 further comprising a positioning receiver connected with said controller, said positioning receiver providing a global position of said positioning receiver to said controller.

6. A system according to claim 4, wherein said spread spectrum data transceiver is selected from a direct sequence spread spectrum data transceiver and a frequency-hopping spread spectrum data transceiver.

7. A system according to claim 4, wherein said identifying means detects at least one of a token, a key, a badge, a password, and a biometric.

8. A system according to claim 1, wherein said client identifier unit further comprises a display connected to said controller and a keyboard connected to said controller.

9. A system according to claim 1, wherein each of said at least one system-access detector comprises:

a controller having an interface board connected with said central computer gateway; and
a spread spectrum data transceiver connected with said controller, said spread spectrum data transceiver communicating data between said controller and at least one of said at least one client identifier unit.

10. A system according to claim 9, wherein said spread spectrum data transceiver is connected to an industrial scientific medical (ISM) band base antenna; and wherein said spread spectrum data transceiver operates in a frequency range from about 900 MHz to about 6 GHz.

11. A system according to claim 1, wherein each of said at least one system-access detector is positioned at a pre-determined distance from another of said at least one system-access detector, said pre-determined distance based on a zone of coverage of each of said at least one system-access detector.

12. A system for authentication and authorization of physical equipment use comprising:
a central computer gateway connected to a WAN;
at least one system-access detector connected with said central computer gateway, each of said at least one system-access detector having a MAC address and an IP address corresponding to a physical location identification; and
at least one client identifier unit having a client identification and located with the equipment, said client identifier unit wirelessly communicating with at least one of said at least one system-access detector.

13. A system according to claim 12, wherein each of said at least one client identifier unit further comprises:
a controller board electrically coupled with the physical equipment;
an operator identification unit connected to said controller board of said client identifier unit;

and

a spread spectrum data transceiver connected with said controller board, said spread spectrum data transceiver communicating data between said controller board and at least one of said at least one system-access detector.

14. A system according to claim 13 further comprising a positioning receiver connected with said controller board, said positioning receiver providing a global position of said positioning receiver to said controller board.

15. A system according to claim 13, wherein said spread spectrum data transceiver is a frequency-hopping spread spectrum data radio.

16. A system according to claim 13, wherein said operator identification unit detects at least one of a token, a key, a badge, a password, a phrase, a fingerprint, a genetic identification, and a retina pattern.

17. A system according to claim 13, wherein said client identifier unit further comprises a display connected to said controller and a keyboard connected to said controller board.

18. A system according to claim 1, wherein each of said at least one system-access detector comprises:

a controller having an interface board connected with said central computer gateway; and

a spread spectrum data transceiver connected with said controller, said spread spectrum data transceiver communicating data between said controller and at least one of said at least one client identifier unit.

19. A system according to claim 1, wherein said computer network comprises a database having at least one of profiles representing each individual user, profiles representing groups of individual users, profiles representing each physical equipment, profiles representing physical areas based on absolute or relative geographic coordinates, and sets of permissions allowing user access to physical equipment.

20. A system according to claim 1, wherein said computer network comprises profiles for a given device configuration, said profiles comprising binary codes to be used by devices defined to the network, and said network providing and modifying said binary codes relating to said devices.

20. A method for authentication and authorization of physical equipment having a control system, said method comprising the steps of:

providing a wireless system for communication between a client identification unit and at least one system-access detector connected to a central computer gateway of a WAN;

connecting the client identification unit with the control system of the physical equipment;

obtaining operator identification at the client identification unit;

transmitting authentication and identification of the client identification unit to the central computer gateway;

transmitting data between the computer network and the central computer gateway; and
permitting activation and monitoring of the physical equipment.

21. A method according to claim 20, wherein said communicating step comprises:

transmitting equipment identification and operator identification of the client identification unit to at least one system-access detector; and

transmitting authentication and identification of the client identification unit between the system-access detector and the central computer gateway.